JURNAL NUANSA INFORMATIKA
Volume 12 Nomor 1, Januari 2018
p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

IMPELEMENTASI ALGORITMA LUC UNTUK PENGAMANAN PESAN BERBASIS ANDROID

Johan Basitu Rahman[1], Muhsin[2], Yati Nurhayati[3]
Fakultas Ilmu Komputer Universitas Kuningan
Jl. Cut Nyak Dien No.36 A, Kel. Cijoho Kuningan 45513
2013081067@student.uniku.ac.id [1], muhsin@uniku.ac.id [2],
yati.nurhayati@uniku.ac.id [3].

Abstrak - Salah satu metode untuk mengamankan data atau informasi adalah dengan menggunakan metode kriptografi. Algoritma LUC adalah metode kriptografi menggunakan dua kata yang berbeda dalam cryptosystem nya. Untuk mengenkripsi bahasa menggunakan file yang memiliki kunci publik, hasil yang dienkripsi dienkripsi file yang aman dari penyusup. Selanjutnya, mendekripsi file yang diproses menggunakan dekripsi menggunakan kunci privat akan mengembalikan file teks yang sama dengan yang asli. Operasi pada algoritma LUC dilakukan dalam domain bilangan, oleh karena itu, sebelum enkripsi dilakukan, teks pertama dikonversi ke bentuk numerik.
Kata kunci: Kriptografi, Algoritma LUC, Enkripsi, Deskripsi

Abstract - *One method for securing data or information is by using cryptography method. The LUC algorithm is a cryptographic method using two different words in its cryptosystem. To encrypt language uses files that has a public key, encrypted results are encrypted files that are safe from intruders. Furthermore, decrypting the processed file using decryption using the private key will return the same text file as the original one. The operation on the LUC algorithm is done in the number domain, therefore, before encryption is done, the text is first converted to numeric form.*

Keywords *: Cryptography, LUC Algorithm, Encryption, Description.*

1. PENDAHULUAN

Penggunaan teknologi telepon genggam (*handphone*) sebagai alat telekomunikasi pada saat ini telah mengubah cara pandang masyarakat dalam berkomunikasi. Telepon genggam mempunyai beberapa fungsi komunikasi yang dapat digunakan antara lain, *video Call, SMS, MMS, Chatting*, Internet, dan lain-lain.

Berkembangnya teknologi telepon genggam dapat dilihat dengan munculnya berbagai sistem operasi yang lengkap layaknya komputer, diantaranya adalah Android. Android adalah sebuah sistem operasi untuk perangkat telepon yang berbasis linux yang menyediakan *platform* terbuka bagi para pengembang untuk menciptakan aplikasi mereka.

Meskipun Android memiliki fitur yang lengkap, namun layanan *SMS* (*Short Message Service*) sebagai layanan pertukaran informasi atau pesan pendek masih menjadi aplikasi komunikasi favorit, karena sampai saat ini semua telepon genggam memiliki layanan ini dan yang paling penting adalah biaya *SMS* relatif murah. Namun demikian *SMS* tidak menjamin integritas dan keamanan pesan yang disampaikan. Pesan yang bersifat personal atau rahasia tidak dijamin sampai ke penerima tanpa diketahui informasinya oleh pihak yang tidak bertanggung-jawab. Beberapa resiko yang dapat mengancam keamanan pesan pada layanan *SMS* antara lain *SMS Snooping*, dan *SMS Interception*.

p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

SMS Snooping terjadi karena kelalaian pengguna telepon seluler. Contohnya ketika seseorang meminjamkan telepon selulernya pada orang lain untuk menggunakan telepon selulernya. Pada saat itu orang tersebut dapat dengan sengaja atau tidak sengaja membuka isi pesan yang ada pada *inbox SMS*.

Kriptografi adalah seni untuk mengamankan informasi dengan menggunakan teknik penyandian. Proses penyandian informasi asli (*plainteks*) yang menghasilkan informasi yang tersandikan (*chiperteks*) disebut *enkripsi*, sedangkan proses menguraikan (*chiperteks*) menjadi informasi asli (*plainteks*) disebut *dekripsi*. Saat ini telah banyak metode kriptografi yang muncul, salah satunya adalah Algoritma Luc, algoritma ini menggunakan dua buah kunci yaitu kunci umum (untuk melakukan enkripsi) dan kunci rahasia (untuk melakukan dekripsi). Operasi pada Algoritma Luc dilakukan dalam domain bilangan, oleh karena itu sebelum dilakukan *enkripsi*, teks terlebih dahulu di konversi kedalam bentuk angka (Saputra *et al.* 2006).

Dengan uraian tersebut maka penulis mengangkat judul "IMPELEMENTASI ALGORITMA LUC UNTUK PENGAMANAN PESAN BERBASIS ANDROID".

2. METODE PENELITIAN

2.1. Kriptografi

Kata-kata "cryptography", "cryptology" dan "cryptanalysis" umunya berubah-ubah dan masing-masing dari kata tersebut memiliki makna yang berbeda. Cryptography yang awal katanya menggunakan kata "crypt", dalam bahasa Yunani kruptos yang artinya sembunyi. Kata terakhir "graphy" mengacu pada arti tulisan. Kriptografi memiliki arti sebagai tulisan yang tersembunyi. (Batten, 2013). Secara umum, kriptografi mengacu pada bagian enkripsi untuk membangun sebuah sistem transmisi rahasia. Sistem transmisi rahasia tersebut merupakan proses enkripsi dalam kriptografi, dimana mengubah plainteks (informasi awal) menjadi cipherteks.

2.2. Algoritma LUC

Menurut Saputra *et al*. (2006) Algoritma Luc merupakan metode kriptografi dengan menggunakan dua kunci yang berbeda dalam kriptosistemnya. Untuk mengenkripsi file teks digunakan fungsi enkripsi yang menggunakan sebuah kunci publik (*Public Key*), hasil enkripsi merupakan file terenkripsi yang aman dari pihak yang tidak berhak atas informasi didalamnya. Selanjutnya untuk membaca file yang telah terenkripsi digunakan fungsi dekripsi dengan menggunakan kunci privat (*Private Key*) yang akan menghasilkan file teks yang sama dengan teks aslinya.

Operasi pada Algoritma Luc dilakukan dalam domain bilangan, oleh karena itu sebelum dilakukan proses enkripsi, teks terlebih dahulu dikonversikan kedalam bentuk angka.

Pada tahun 1993, Smith dan Michael menyatakan bahwa algoritma LUC merupakan algoritma yang dijabarkan dari deret Lucas. Sehingga didapat rumus enkripsi dan dekripsi dari barisan lucas tersebut.

Algoritma LUC mempunyai ciri khas dari algoritma kriptografi asimetri yang lain, dimana setiap katakter dari string berupa teks atau plainteks yang dimasukkan, lalu dikonversi kedalam bentuk bilangan dengan kode ASCII *(American Standard Code for Information Interchange).*

2.2.1. Perhitungan Certainty Factor

Dalam menyelesaikan algoritma Luc terdapat tiga tahap utama yaitu algoritma pembangkitan kunci, proses enkripsi dan proses dekripsi.

1. Algoritma pembangkitan Kunci

p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

A. Algoritma Kunci Publik

1. Pilih dua bilangan prima sebarang, misal *p* dan *q* dimana $p \neq q$.
2. Hitung nilai $N = p \times q$. Nilai *N* akan digunakan dalam menghitung modulo pada proses enkripsi dan dekripsi.
3. Hitung semua bilangan yang relatif prima terhadap (*p*-1), (*p*+1), (*q*-1) dan (*q*+1).
4. Pilih salah satu bilangan secara acak dari hasil yang didapatkan pada poin (c) sebagai kunci publik *e*.

B. Algoritma Kunci Privat

a) Masukkan dua bilangan prima *p* dan *q*.
b) Masukkan *e* yang dihitung pada tahap pembangkitan kunci public.
c) Hitung determinan $D = C^2 - 4$.
d) Cari simbol legendre dari $\frac{D}{p}$ dan $\frac{D}{q}$.
e) Hitung nilai $S(N) = LCM\left[\left(p - \frac{D}{p}\right), (q - \frac{D}{p})\right]$.
f) Hitung $ed \equiv 1 \bmod S(N)$.

2. Proses Enkripsi

Proses Enkripsi Proses enkripsi adalah proses pengacakan data atau pesan, misalkan A akan bertukar informasi dengan B, pihak A dan B sama-sama melakukan pembangkitan kunci seperti yang telah dijelaskan pada sub bab sebelumnya, kemudian A dan B bertukar kunci public (A menerima kunci public dari B dan B menerima kunci public dari A) dimana pertukaran kunci tersebut tidak bersifat rahasia. Dalam proses enkripsi dimisalkan B ingin mengirim data atau pesan kepada A, maka B terlebih dahulu harus mempunyai kunci public (*e*) yang diberikan oleh A. Selanjutnya proses enkripsi dapat dijelaskan sebagai berikut :

1) Plainteks (M) adalah isi pesan atau informasi yang akan disampaikan oleh B kepada A.
2) Nilai *e* dan *N* didapatkan dari kunci public yang telah diberikan A kepada B.
3) Plainteks (M) yang akan disampaikan kepada A dipecah atau diatur menjadi blok-blok *m1*, *m2*, …*mi* yang mempunyai dua karakter pada tiap blok.
4) Setiap blok yang telah didapatkan (*mi*) di ubah dalam bentuk ASCII kemudian di enkripsi dengan persamaan $ci = V_e\ (M_i\ ,\ 1) \bmod N$.
5) Setiap blok yang telah dienkripsi (*ci*) digabungkan kembali sehingga menjadi sebuah chiperteks yang utuh (C).

3. Proses Deskripsi

Proses dekripsi sebuah chiperteks hampir sama dengan proses enkripsi sebuah pesan, perbedaannya adalah persamaan yang dipakai adalah $mi = V_d\ (C_i\ ,\ 1)\ mod\ N$ serta kunci yang dipakai adalah kunci dekripsi (*d*,*N*) dimana kunci tersebut telah di ketahui pada proses pembangkitan kunci. Misalkan A telah menerima chiperteks (C) dari B dengan menggunakan kunci public yang telah diberikan kepada B, maka langkah-langkah dekripsi adalah sebagai berikut :

1) Chiperteks (C) adalah isi pesan atau informasi yang telah dienkripsi oleh B dan diterima oleh A.
2) Nilai *N* didapatkan dari kunci privat yang telah dicari pada tahap pembangkitan kunci.
3) Chiperteks yang telah diterima dari B dipecah atau diatur menjadi blok-blok C_1, C_2, … *ci* yang mempunyai dua karakter pada tiap blok.
4) Setiap blok yang telah didapatkan (*ci*) di ubah dalam bentuk ASCII.
5) Hitung nilai deskriminan $D = C^2 - 4$.
6) Cari simbol legendre dari $\frac{D}{p}$ dan $\frac{D}{q}$.
7) Hitung LCM $\left(p - \frac{D}{p}, q - \frac{D}{q}\right)$.
8) Cari nilai *d* dari $ed \equiv 1 \bmod S(N)$.
9) Gunakan *d* dalam persamaan dekripsi $m_i = V_d\ (C_i\ ,\ 1)\ mod\ N$.

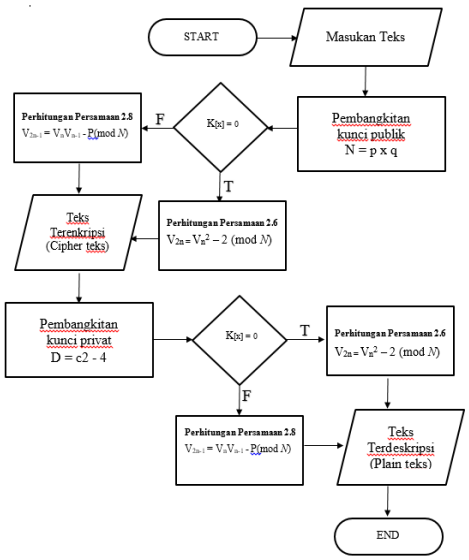
p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

10) Setiap blok yang telah didekripsi (*mi*) digabungkan kembali sehingga menjadi sebuah plainteks yang utuh (M)

3. HASIL DAN PEMBAHASAN

3.1. Flowchart

3.1.1. Flowchart Algoritma LUC



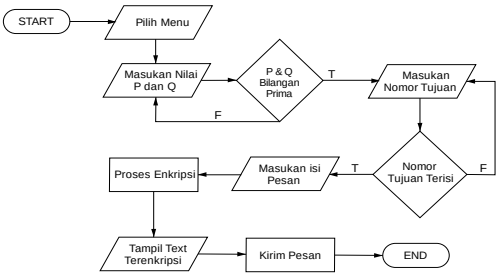
Gambar 1. flowchart Algoritma LUC

Alur langkah dari flowchart Algoritma LUC diatas adalah sebagai berikut:

1. Memasukan teks (Plainteks).
2. Pembangkitan Kunci Publik, dimana nilai P dan Q dibutuhkan untuk membuat kunci public.
3. Jika Kx = 0 maka dihitung oleh persamaan 2.6, tetapi jika Kx = 1 maka dihitung oleh persamaan 2.8
4. Dalam perhitungan tersebut teks asli dikonversi ke dalam kode ASCII.
5. Setelah perhitungan dan konversi selesai, maka didapatkan *Ciphertek*s atau teks yang terenkripsi.
6. Untuk proses deskripsi, teks yang terenkripsi di hitung dan konversi kembali ke dalam kode ASCII, setelah selesai, maka didapatkan kembali teks yang asli atau *Plainteks*.

3.1.2. Flowchart Sistem Tulis Pesan

Dalam pembuatan aplikasi ini digunakan algoritma luc sebagai metode kriptografi untuk pengamanan teks pesan. Berikut flowchart sistem tulis pesan pada aplikasi keamanan pesan :



Gambar 2. flowchart sistem tulis pesan

Alur langkah dari *flowchart* sistem tulis pesan pada gambar 2 adalah sebagai berikut:

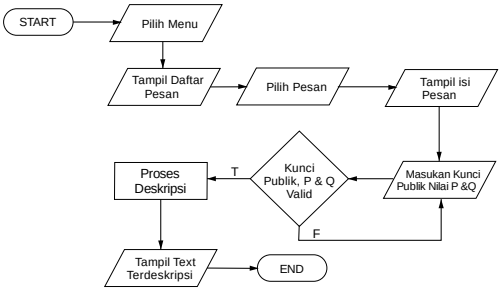
1. Memilih menu tulis pesan di halaman utama.
2. Memasukan nilai P dan Q untuk pembuatan kunci publik.
3. Jika P dan Q bilangan prima dan lebih dari nilai yang ditentukan maka sistem melanjutkannya ke halaman tulis pesan, tetapi jika nilai P dan Q salah, maka sistem memunculkan alert dan user harus mengulanginya kembali.
4. Jika nomor tujuan terisi lanjutkan dengan menulis isi pesan, tetapi jika nomor belum terisi sistem akan memunculkan alert dan user harus memasukan nomor tujuan.
5. Proses enkripsi dilakukan ketika nomor tujuan dan isi pesan sudah terisi, proses ini dilakukan oleh algoritma LUC.
6. Setelah melakukan proses enkripsi sistem mengirimkan isi pesan.

3.1.3. Flowchart Sistem Pesan Masuk

Dalam pembuatan aplikasi ini digunakan algoritma luc sebagai metode kriptografi untuk pengamanan teks pesan. Berikut

p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

flowchart sistem pesan masuk pada aplikasi keamanan pesan :



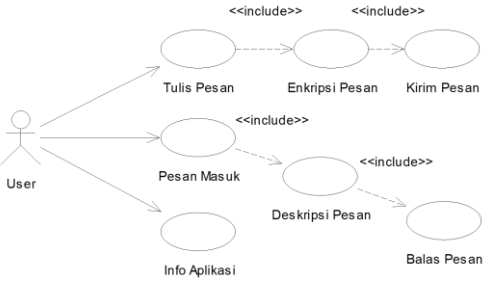
Gambar 3. flowchart sistem pesan masuk

Alur langkah dari *flowchart* sistem tulis pesan pada gambar 3.3 adalah sebagai berikut:

1. Memilih menu pesan masuk di halaman utama.
2. Sistem menampilkan daftar pesan masuk.
3. User memilih pesan terenkripsi yang diterima.
4. Sistem menampilkan pesan terenkripsi serta tanggal dan waktu pesan tersebut diterima.
5. Masukan nilai kunci publik, nilai P dan nilai Q.
6. Ketika kunci publik benar maka sistem akan melanjutkan pada proses deskripsi pesan, tetapi jika kunci publik, nilai P dan nilai Q tidak benar, maka sistem akan memunculkan alert dan user harus memasukan ketiga nilai tersebut dengan benar.
7. Proses deskripsi dilakukan oleh algoritma LUC.
8. Setelah proses deskripsi selesai, sistem akan menampilkan teks asli dari pesan yang terenkripsi.

3.2.Use Case Diagram

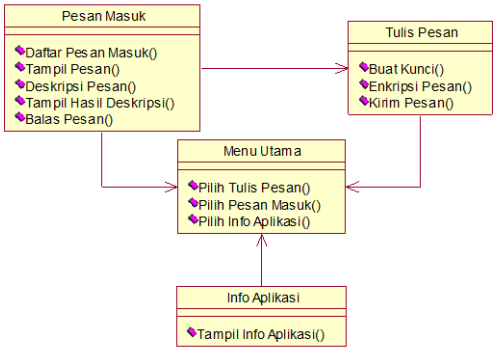
Digunakan untuk memodelkan atau menggambarkan batasan sistem dan fungsi - fungsi utamanya. Mesdeskripsikan fungsi dari sebuah sistem dari perspektif pengguna, use case bekerja dengan cara mendeskripsikan tipikal interaksi antara pengguna sebuah sistem dengan sistemnya sendiri. Didalam sistem terdapat pengguna yaitu pemakai aplikasi. Peran aktor yang ada dapat terlihat pada diagram Use Case pada gambar Gambar 4



Gambar 4. use case diagram sistem

3.3.Class Diagram

Diagram kelas atau class diagram merupakan sebuah spesifikasi yang saling berhubungan dan membentuk sebuah objek. Dibawah ini merupakan gambaran dari diagram kelas dari game pertanian yang identigifikasi kelas-kelas yang dibutuhkan untuk menghadirkan objek-objek yang digunakan dalam pembangunan game pertanian ini. Setiap kelas yang dibuat memiliki hubungan relasi dengan kelas lainnya.



Gambar 5. *Class* Diagram Aplikasi

3.4 Antarmuka Halaman Utama

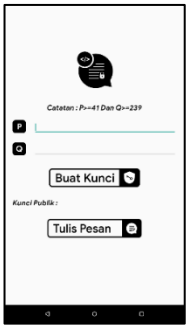
Pada halaman utama ini menampilkan button yang di gunakan sebagai navigasi ke halaman berikutnya seperti terlihat pada gambar 6. dibawah ini.

p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

Gambar 6. Halaman Utama

Dihalaman ini terdapat satu *ImageView* dan tiga *button, button Tulis Pesan* adalah *button* untuk berpindah ke halaman pembuatan kunci dan tulis pesan, b*utton Pesan Masuk* adalah *button* untuk melihat pesan masuk dan mendeskripsikan pesan yang dipilih pada daftar pesan masuk, *button Info Aplikasi* adalah *button* untuk menuju halaman informasi aplikasi.

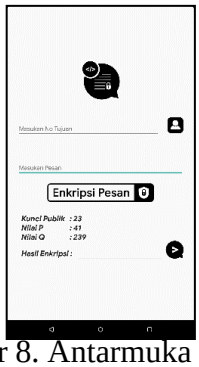
3.5 Antarmuka Pembuatan Kunci Publik



Gambar 7. Antarmuka Pembuatan Kunci Publik

Sebelum pengguna melakukan penulisan pesan dan mengenkripsikan isi pesan, terlebih dahulu pengguna diarahkan untuk membuat kunci publik, sesuai dengan aturan algoritma LUC dan kebebasan pengguna untuk memilih nilai dari kunci publik.

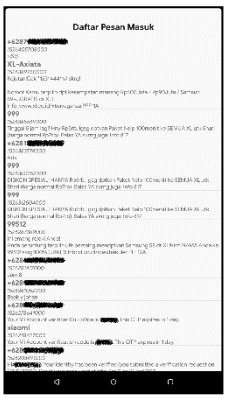
3.6 Antarmuka Tulis Pesan



Gambar 8. Antarmuka Tulis Pesan

Dihalaman ini pengguna melakukan pengisian nomor tujuan, menulis pesan, mengenkripsi pesan dan melakukan pengiriman pesan, hasil dari enkripsi pesan akan ditampilkan didalam *form hasil enkripsi.*

3.7 Antarmuka Daftar Pesan Masuk



Gambar 9. Antarmuka Daftar Pesan Masuk

Di halaman ini terdapat beberapa pesan masuk, dimana pengguna bisa memilih pesan yang akan dilihat dan dideskripsi dengan meng*klik* pesan tersebut.

3.8 Antarmuka Lihat Pesan Masuk

Gambar 10. Antarmuka Lihat Pesan Masuk

p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

Dihalaman ini terlihat detail pesan yang dipilih dari daftar pesan yang masuk seperti nomor pengirim, tanggal serta waktu yang diterima, dan isi dari pesan yang terenkripsi.

3.9 Antarmuka Deskripsi Pesan

Gambar 11. Antarmuka Deskripsi Pesan

Didalam halaman ini, pengguna memasukan kunci public, nilai P dan Nilai Q, sebelum pengguna menekan tombol deskripsi pesan, hasil dari deskripsi pesan akan ditampilkan didalam *form hasil deskripsi*, pengguna juga bisa membalas pesan tersebut dengan cara memilih tombol Balas Pesan.

4 KESIMPULAN

Berdasarkan hasil implementasi dan pengujian, maka kesimpulan yang dapat diperoleh dari hasil penelitian skripsi ***"Implementasi Algoritma LUC Untuk Pengamanan Pesan Berbasis Android "*** adalah sebagai berikut :

1. Algoritma LUC dapat diimplementasikan pada ponsel berbasis android, sebagai sistem keamanan pesan.
2. Aplikasi yang dibangun, terbukti mampu mengenkripsi pesan dan mengirimkan pesan terenkripsi serta mendeskripsikannya, terutama untuk huruf kapital.

5. SARAN

Adapun saran-saran yang ingin disampaikan adalah :

1. Menyempurnakan aplikasi ini agar dapat melakukan enkripsi dan deskripsi dengan lebih baik terutama untuk karakter kecil.
2. Meminimalisir atau menghilangkan batasan nilai untuk pembuatan kunci publik, dan maksimal teks atau karakter yang dimasukan.
3. Menambahkan *database* untuk menyimpan kunci publik yang telah dibangkitkan, hal ini disebabkan penulis belum mampu menambahkan *database* berkaitan dengan keterbatasan kemampuan penulis dalam bahasa *Java*.
4. Menambahkan beberapa fitur yang dapat mempermudah penggunaan aplikasi, seperti *auto insert* nomor telepon, *auto insert* kunci.

DAFTAR PUSTAKA

Saputra, R., Yismianto, B., dan Suhartono. 2006. "*Kriptografi Teks Dengan Menggunakan Algoritma LUC"*. Skripsi. Semarang : Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Diponegoro.

Usman, Nurdin. (2002). "*Konteks Implementasi Berbasis Kurikulum*". Jakarta:PT. Raja Grafindo Persada.

Batten, 2013. "*Applications and Attacks",* Public Key Cryptography: The Institute of Electrical and Electronics Engineers, Inc.